

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF WEST VIRGINIA

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
APPLE ACCOUNT

jarrod.p.richards@gmail.com

THAT IS STORED AT PREMISES  
CONTROLLED BY APPLE, INC.

Case No. 1:19mj65

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, JAMES ROGERS, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with the following: jarrod.p.richards@gmail.com (the "Subject Account"), which is stored at premises controlled by Apple Inc., a technology provider headquartered at 1 Infinite Loop, Cupertino, CA 95014. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple, Inc. to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation since February 23, 2003. Your Affiant is a duly authorized Federal law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), and is empowered by law to conduct investigations of and to make arrest for offenses enumerated in Title 18, U.S.C. § 2516. Your

Affiant has experience investigating criminal matters including white collar crime, violent crimes, and other violations of Federal law. Your Affiant has knowledge of or participated in all investigative activities in this investigation. The information provided in this Affidavit is based upon investigation conducted by the FBI, Wheeling, West Virginia Resident Agency.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. § 1348 - Securities and Commodities Fraud, Title 18 U.S.C. § 1343 - Wire Fraud, and Title 18 U.S.C. § 1956 - Money Laundering have been committed by PHILLIP WAYNE CONLEY. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities and fruits of these crimes further described in Attachment B.

#### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

#### **PROBABLE CAUSE**

6. This investigation was opened on January 25, 2017 after the United States Attorney’s Office, Northern District of West Virginia contacted the FBI about a securities fraud investigation that was brought to their attention by the West Virginia State Police. The fraud investigation involves, PHILLIP WAYNE CONLEY d.b.a., ALPAX, LLC, originally based out of Morgantown, West Virginia. CONLEY has had previous employment with various banks and

financial institutions including Merrill Lynch, Citibank and Bank of America before starting his own consulting company, ALPAX, LLC. CONLEY had his securities license in West Virginia suspended as of December 2015. According to the WV Secretary of State, ALPAX, LLC is registered as a real-estate and technology investment company. CONLEY also appears to be operating a business called ALPAX HOLDINGS, LLC, but it is not registered with any state agency.

7. On or about May 2018, the FBI began receiving complaints from various individuals claiming that they invested money with CONLEY in various investment products including real-estate development and power plants. CONLEY developed associations with various churches and other potential investors in the community and told them that his company ALPAX, LLC, was investing in very lucrative real-estate development projects involving student housing for universities. CONLEY told investors that their money would be invested for a period of one year to as much as three years and would generate dividends in excess of eight per cent (8%). In some cases, investors were not told exactly what their investment would be invested in, but Conley told them that his company ALPAX, LLC would be managing their investment. All of the investors trusted CONLEY after spending time with him or after CONLEY was recommended by friends, family or colleagues who had previously invested with ALPAX, LLC.

8. CONLEY was able to gain the trust and loyalty of investors through an elaborate scheme to present the image or façade of great financial wealth and success. CONLEY perpetrated this façade through establishing business offices with hired staff, and traveling regularly on private planes. CONLEY told investors that he owns expensive homes and condos, including a condo at the Ritz Carlton Hotel in Washington D.C. CONLEY also traveled to various political fundraisers and vacations in private jets, which he claimed to have part ownership of. On occasion, CONLEY

would pay for other friends and investors to travel with him on these trips and vacations to lavish locations, such as Hialeah, Florida. CONLEY wore expensive clothes and jewelry and drove very expensive cars and he told investors that he had a background in business and finance and attended various institutions of higher learning including West Virginia University and Wharton Business School. CONLEY claimed to have various business and personal connections with U.S. Senators, Governors, including the former Governor of Indiana, Mike Pence, and CONLEY claimed to have millions of dollars of assets invested in coal and oil. CONLEY told several investors that he was involved in other business ventures and partnerships with the Koch brothers, which your Affiant is able to refute.

9. From May 2018, to present, the FBI has identified approximately twenty victim investors. The investors have very similar stories relating to CONLEY and his purported wealth and success. The investors were told that CONLEY would manage their investments through his company ALPAX, LLC and in most cases, CONLEY sent quarterly dividend sheets to investors that showed the growth of their investment. It wasn't until investors were not receiving dividend updates or were having difficulties contacting CONLEY to recover their money, that they began suspecting that CONLEY was a fraud and con man. CONLEY in most cases would use stall tactics to explain to investors why their money could not be returned and in some cases CONLEY would send investors paperwork to fill out in order to return their money, but CONLEY never returned their money after completing the paperwork. Investors have been able to maintain contact with CONLEY through phone or text, but never knew for certain where he was living at any given time, because CONLEY moved around frequently. The investors were unable to recover their investment money with very few exceptions. The total amount of money invested with CONLEY and ALPAX, LLC is approximately five million dollars. A review of financial documents reaffirms

suspicious that CONLEY used the investment money in support of a lavish lifestyle of travel, expensive luxury rental accommodations and vacations, jewelry, expensive vehicles, private jets, clothing, fine dining and other personal expenses. Some of the investor money was used for initial business leases, employee salaries and other expenses, but based on financial analysis, none of the money was legitimately invested in any financial investment instruments by CONLEY, ALPAX, LLC or its affiliates.

10. During the course of the investigation, your Affiant learned through victim and witness interviews, that CONLEY exhibited a pattern of default on leases, rental properties, lines of credit and contracts. CONLEY owes substantial amounts of money to investors, landlords, leasing companies, vacation and resort rental property management companies, a home relocation service, employee salaries, and a construction company. CONLEY would disappear when confronted or contacted about defaulting on these various responsibilities and CONLEY would move somewhere else and start the same pattern over again. In October 2018, CONLEY was arrested in Florida for attempting to skip out on the bill for a luxury property rental. Your Affiant also learned that CONLEY has outstanding debt with other individuals not related to ALPAX, LLC investments, which he accrued through similar means of deception and fraud. One individual who rented a house to CONLEY was sued for various construction projects that were completed on his home that were contracted by CONLEY. These construction companies sued the owner and CONLEY moved away leaving the debt unpaid. Your Affiant learned that CONLEY was evicted from numerous rental properties for failing to pay rent, but he would just get a moving truck and move to another location and get another lease set up without paying his other debts. CONLEY even failed to pay for expensive tuition for his son to attend elite educational institutions in Indiana and New York and again, CONLEY moved away to another location and continued the pattern of

deception and fraud. Throughout the investigation, CONLEY has maintained contact with investors and continues to ensure them that their investments are secure and performing well.

11. In August 2018, the FBI interviewed R.F., owner of the office building located at 125 Worth Avenue, Palm Beach, Florida 33401. R.F. advised that he rented Suite 300 to CONLEY, but CONLEY defaulted on the lease and stopped coming to the office. R.F. followed protocol for abandonment of the business equipment and property CONLEY left at the office suite and later turned over items related to ALPAX, LLC to the FBI. R.F. advised that prior to signing a lease, CONLEY told him he was in the hedge fund business and wanted to expand. R.F. required CONLEY to produce a financial statement and CONLEY provided a financial statement that showed he had over \$100 million dollars in assets. R.F. thought CONLEY and his partner J.R. would be good tenants and offered CONLEY the lease.

12. In January 2019, I interviewed CONLEY'S former Administrative Assistant, J.R. J.R. advised that he worked for CONLEY and prepared ALPAX, LLC dividend statements for investors on his company laptop, an Apple MacBook Pro. J.R. designed the dividend statements and all the information he put on the statements was provided by CONLEY. J.R. never saw any ALPAX, LLC financial statements and only prepared documents for CONLEY with information directly provided by CONLEY. J.R. also made travel arrangements for CONLEY for his business trips. J.R. advised that the computer he used for ALPAX, LLC business purposes was at the ALPAX, LLC office, 125 Worth Avenue, Suite 300, Palm Beach, Florida 33401. J.R. advised that he also performed business functions for ALPAX, LLC utilizing a Gmail login and password for their business iCloud account. According to J.R., the iCloud account contains other documents and business records pertaining to ALPAX, LLC, including investor information. J.R. was provided a user login and password to access the iCloud account. J.R. provided the user ID and password for



the iCloud account to the FBI. J.R. advised that he believed CONLEY was a legitimate investment manager and businessman and had no reason to doubt him, until J.R. started hearing investor complaints. J.R. never saw any financial statements for ALPAX, LLC, so he was not aware of the financial status of ALPAX, LLC or CONLEY. J.R. also invested his personal savings with CONLEY in ALPAX, LLC, but has not been able to recover his money.

13. The items that were received from R.F. from 125 Worth Avenue, Suite 300, Palm Beach, Florida 33401 include: One Apple 13inch MacBook Pro serial number C02WJ0ZWHV22, one G/Drive Mobile USB serial number 7DG25NZB, one SoundLogic/XT Blue External Drive, one 32G Ipad serial number GG7WL1RZJF88 Model A1954, and one box of various ALPAX, LLC business documents. These items, in addition to the iCloud account login and password which was provided by J.R., were used by CONLEY and J.R. for business operations pertaining to ALPAX, LLC.

14. Based on the aforementioned and statements provided by J.R., I believe there is probable cause that the iCloud account used by CONLEY and J.R. for ALPAX, LLC, contains fruits and instrumentalities of the crimes alleged against CONLEY and ALPAX, LLC in this affidavit. This affidavit seeks authority to execute a search warrant of the iCloud account identified in Attachment A of this affidavit for items described in Attachment B of this affidavit.

### **INFORMATION REGARDING APPLE ID AND iCloud<sup>1</sup>**

15. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

16. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

---

<sup>1</sup> The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at [https://www.apple.com/business/docs/iOS\\_Security\\_Guide.pdf](https://www.apple.com/business/docs/iOS_Security_Guide.pdf), and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.



d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS.

Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

17. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

18. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

19. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the

account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

20. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

21. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications

between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

22. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

23. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

24. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

25. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with any yet unidentified victims. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of instrumentalities of the crimes under investigation.

26. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

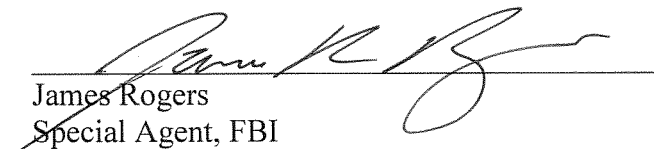
27. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment

B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

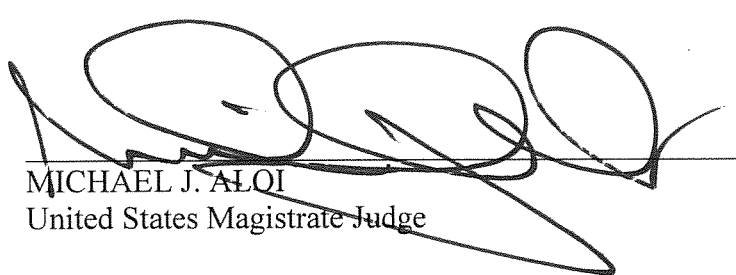
**CONCLUSION**

28. Based on the forgoing, I request that the Court issue the proposed search warrant.

29. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

  
James Rogers  
Special Agent, FBI

Sworn and subscribed before me on this 1 day of May, 2019.

  
MICHAEL J. ALQI  
United States Magistrate Judge